UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/327,477	06/08/1999	YASUTSUGU KURODA	826.1547/JDH	5479

21171   7590   03/18/2003

STAAS & HALSEY LLP
700 11TH STREET, NW
SUITE 500
WASHINGTON, DC   20001

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-26_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-26_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____

Response to Remarks

In response to amendment received on 30 December 2002, it is acknowledged

that the changes to the claims 1-7 and 9-19 and the addition of claims 22-26 do not

introduce new matter.

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

2.   Claims 2, 22 and 26 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

3.   Referring to claim 2, this claim is rejected for there is no antecedent basis for "the

group".

4.   Referring to claim 22, this claim is rejected for containing "when performing an

encrypting encryption process on electronic data" which is an unclear statement.

Appropriate correction is necessary.

5.   Referring to claim 26, this claim is rejected for containing "wherein the method is

performed by a data storage apparatus data transmission comprising a transmission to

a data storage device..." which is unclear language. Appropriate correction is

necessary.

Response to Arguments

6.   Applicant's arguments received on 30 December 2003 have been fully

considered but they are not persuasive.

7.   With respect to claims 1-5, 8-9, 11-12, 17-18 and 20-21, applicant on page 9, line

5, argues that "there is nothing in Kuroda that discusses selection keys based on the

destination".

Kuroda discloses a secure system of electronic data storage apparatuses for

safely storing and transmitting data between storage apparatuses (col. 1, lines 6-29 and

lines 44-55, col. 2, lines 30-40, col. 4, lines 56-64 and col. 7, lines 45-55). Unique

individual key assigned to each electronic data storage and a master key (group key)

common to the plurality of electronic data storage apparatuses are used for storing data

in electronic data storages and transmission of data between storages, respectively

(col. 3, lines 29-34, col. 4, lines 8-10 and col. 9, lines 26-35). Additionally, Kuroda

discloses secure communication among secure electronic data storages located in

different locations (networks) over the Internet (Fig. 36 and col. 21, lines 12-27) using

public key encryption method (col. 1, lines 20-24 and col. 22, lines 53-55). In Kuroda

system, each electronic data storage apparatus is identified by identification information

for uniquely identifying each of the electronic data storage apparatuses (col. 4, lines 8-

21), which is used for transferring data from a source to an electronic data storage

apparatus destination (col. 4, lines 22-31). Thus, contrary to the applicant's arguments

Kuroda uses an individual key for guaranteeing the security of the stored data in an

electronic data storage, a common key (group key) to transfer data among the

electronic data storage apparatuses in a group and a public key system to transmit

electronic data over the Internet to another electronic data storage as it is well-known in

the industry.

8.   With respect to claims 5-7, 10-16, and 19, applicant on page 9, lines 6 and 7,

argues "Mittra adds nothing to Kuroda with respect to the features of the invention

discussed above".

On the contrary, Mittra discloses a system for secure group communication with

hierarchical structure that uses a group key for encrypting messages transmitted

between the group members (col. 2, lines 8-20, col. 4, lines 6-16, col. 6, line 67-col. 7,

line 14 and col. 13, lines 4-5), a member key for private conversation with each member

(col. 7, lines 52-59, col. 8, lines 61-65, col. 10, lines 15-17 and col. 14, lines 39-42) and

a public key method for message transmission over the Internet (col. 4, lines 57-64, col.

5, lines 18-26 and lines 42-46, and col. 9, lines 54-62).

Examiner contends that a person of ordinary skill in the art would be motivated to

combine the teaching of a hierarchical structure of electronic data storage apparatuses

as taught in Mittra with the electronic data storage system of Kuroda because it would

provide a system in which the distribution and security of information and encryption

keys are centrally managed and controlled for a plurality of groups of electronic data

storage apparatus. Furthermore, examiner contends that the combined Kuroda and

Mittra would establish a *prima facie* case of obviousness with regard to claims 5-7, 10-16, and 19.

9.   However, based on the above submission, examiner maintains the previous rejection.

10.   Applicant on pages 6-8 has introduced new claims 22-26. However, these claims do not add any new matter to the previous claims and are rejected as being anticipated by Kuroda as applied to like elements of claims 1-5, 8-9, 11-12, 17-18 and 20-21 and the following:

11.   With respect to the added new claim 22, Kuroda discloses all the elements introduced in this claim, which are identical to the same elements in claim 1. Thus, this claim is rejected as applied to like elements of claim 1 stated in the Office Action dated September 20, 2002.

11.   With respect to the added new claim 23, Kuroda discloses the use of a computer program to be installed on a personal computer having the functions of storing electronic data, encrypting data for storing and transmission to other computer, and selecting the corresponding encryption key for the intended purpose (col. 3, line 65-col. 5, line 8 and col. 15, lines 19-32).

12. With respect to claims 24-26, these new claims are rejected as applied to like elements of claims 17-19 stated in the Office Action dated September 20, 2002 and the following:

Kuroda discloses a data transmission method through a network whether a local area network or Internet (local environment or global environment) (col. 1, lines 44-50, col. 7, lines 51-57, col. 21, lines 14-25, and col. 22, lines 53-55). In the Kuroda system, each electronic data storage apparatus is identified by identification information for uniquely identifying each of the electronic data storage apparatuses (col. 4, lines 8-21) that is used for transferring data from a source to an electronic data storage apparatus destination (col. 4, lines 22-31). The identification information of the electronic data storage corresponds to the recited indicator that is the device (computer) address (i.e., an IP address which is common in the industry). Kuroda, also, discloses that for the transmission of data to an electronic data storage device, the data is encrypted using the unique individual key of the storage (device) (col. 8, lines 47-53, col. 12, lines 61-65, and col. 14, lines 1-4 and lines 26-31).

Previous Rejection:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2.   Claims 1-5, 8, 9, 11, 12, 17, 18, 20, 21are rejected under 35 U.S.C. 102(e) as being anticipated by Kuroda et al. (6,421,779 B1) (hereinafter Kuroda).

3.   Referring to claim 1, Kuroda discloses an electronic data storage apparatus having key management means (Fig. 13, and col. 9, lines 26-28) for managing the data storage's unique individual key (col. 9, line 30) and the key shared by all the data storages in the group (a master key similar to common key) (col. 1, lines 23-24.) It is also discloses in the Kuroda's system that there exist encryption means that use individual key for encrypting stored data in the electronic data storage and use the shared common key to encrypt the electronic data for the purpose of transmission to another storage (Figs. 6, No. 3 and 4, col. 1, line 47, col. 2, lines 31-36, col. 7, lines 51-53, col. 11, lines 5-10, and col. 12, lines 59-62.)

4.   Referring to claim 2, Kuroda teaches the use of an individual key (as group key) shared among the data storages (col. 1, lines 23-24, col. 2, lines 21-22, and col. 5, lines 50-51) and a unit for managing the individual key (Figs. 11, 13, and 39.)

5.   Referring to claim 3, Kuroda teaches the use of an authorization function (Fig.

21) which can be implemented as a main data storage apparatus. This authorization

function generates the individual key (Fig. 16, S37) and distributes it to each data

storage apparatus (col. 3, lines 29-30.) The individual key is generated (col. 11, lines

22-25) using an identifier of the electronic data storage apparatus, which can be

replaced by the individual key of the main electronic data storage apparatus.

6.   Referring to claim 4, Kuroda teaches the use of an authorization function (Fig.

21) which can be implemented as a main data storage apparatus in the group of data

storages. This authorization function generates the group key (master key) (Fig. 15, S6)

and distributes it to each data storage apparatus (col. 3, lines 1-3, col. 4, lines 8-10.)

The master key is generated (col. 11, lines 22-25) using an identifier of the electronic

data storage apparatus, which can be replaced by the individual key of the main

electronic data storage apparatus.

7.   Referring to claim 5, Kuroda teaches the use of an authorization function as

stated above to generate a group key similar to main electronic data storage. This

generation process of group key can use the individual key of the main electronic data

storage preliminary assigned to it (col. 3, lines 51-55, and col. 4, lines 32-36.)

8.   Referring to claim 8 and 9, Kuroda teaches the use of identification information

assigned to each electronic data storage (col. 3, lines 51-55.) This unique identification

information can be the storage preliminary individual key (col. 4, lines 32-36) that can be

used to generate the electronic data storage apparatus individual key. Also, Kuroda

discloses the use of an authentication information generation unit of the electronic data

storage (Fig. 16, S37 and col. 12, lines 56-65.) to generate authentication information using master or individual key. This process can be performed using the data storage individual key to encrypt the information identification of the group to generate the group key and distributed to the group's electronic data storages.

9.   Referring to claims 17 and 18, Kuroda discloses a system of electronic data storage apparatus consisting of units for storing the individual and common keys at the electronic data storage and transmitting data to another data storage (Figs. 11 and 14.) The data storage has apparatuses to communicate to another electronic data storage, transfer data, and using individual key to encrypt data for storing data at the storage, in order to provide the security of data. The data mutually authenticated to meet the recitation of encryption during the transmission step using a common key shared among the electronic data storage apparatuses (col. 1, lines 44-55.)

10.   Referring to claims 20 and 21, Kuroda teaches the use of a computer program to be installed on a personal computer to receive and store data in an electronic data storage, to verify data, and transfer data to another data storage (col. 1, lines 9-17, and Figs. 16, 17, and 23.) As mentioned above, unique individual and common keys are used for storing data in the electronic data storage, transferring data to another storage, and verification of data.

Claim Rejections - 35 USC § 103

11.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12.   Claims 5-7, 11-16, and 19 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kuroda et al. (6,421,779 B1) (hereinafter Kuroda) in view of Mittra

(5,749,736).

13.   Referring to claims 5, 6, 7, and 10, Kuroda does not teach the use of a main

electronic data storage in each group to generate the group (common) key and to

distribute it among the group members and a management apparatus to manage the

main data storages and generate group key and a master key to be used by all the data

storage apparatuses. Mittra teaches the use of a computer to act as the main member

(Trusted Intermediary: TI) in each group (col.12, line 67) to change (generate) the group

key and transmit to other members in the group (col. 13, lines 49-53, and col. 12, lines

1-15.) Also, Mittra uses a group security controller (GSC) (col. 4, lines 5-19, col.3, lines

35-42, and col. 12, lines 5-15) that manages all the groups, generates group keys and a

key (master key) to be shared among all groups and transmits them to the main

members (TI) of each group. It would have been obvious to one of ordinary skill in the

art at the time the invention was made to add the scheme of Mittra to the Kuroda's

system because it would provide for a group of electronic data storages a main member

to change the group's common key when ever it is needed and an apparatus at the top

of the system to control and manage the main members of the groups. This would

decrease the traffics among the electronic data storage apparatuses and would

increase the group independence.

14.   Referring to claims 11, and 12, Kuroda teaches the use of identification

information assigned to each electronic data storage (col. 3, lines 51-55.) This unique

identification information can be the storage preliminary individual key (col. 4, lines 32-

36) that can be used to generate the electronic data storage apparatus individual key.

Also, Kuroda discloses the use of an authentication information generation unit of the

electronic data storage (Fig. 16, S37 and col. 12, lines 56-65.) to generate

authentication information using master or individual key. This process can be

performed using the data storage individual key to encrypt the information identification

of the group to generate the group key and distributed to the group's electronic data

storages.

15.   Referring to claims 13-16 and 19, Kuroda does not teach the use of a

hierarchical structure to manage the groups of the electronic data storage apparatuses

in a higher and lower levels fashion and the group key to be dependent upon a

hierarchical level of group. Mittra teaches the use of a hierarchical order for the groups

(col. 12, lines 30-60, and Fig. 1) to manage the groups and the group keys. In this

system of Mittra as shown in Fig. 1 there is a member (TI) at a higher level group that

control and manages the lover level group(s). The communication (transmission of data)

from a member at the higher level group to a member at a lower level group is done

through the TI of the group at the higher level to the TI of the group at the lower level

group and finally to the targeted member at the lower level group and vice versa. The

individual, group, and public keys are used (col. 4, lines 33-36) to encrypt and decrypt

the data when data is stored in a data storage, transferred to a another storage within group, or transferred to a storage in a different group. Also, the TI at a higher level group changes the group key for the TI at a lower level group (col. 4, lines 5-25, and col. 13, lines 48-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the hierarchical scheme of Mittra to the Kuroda's system because it would provide a scalable electronic data storage apparatuses system that would make the group more manageable and to transmit data and encryption keys among the groups and the electronic data storages with a higher security and efficiency.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.
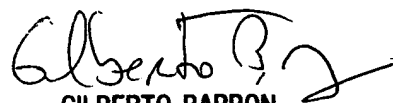
Abdulhakim Nobahar

March 13, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100